tenable | Data Sheet

AI Security Posture Management (AI-SPM)

Securing AI resources and data in the cloud with Tenable Cloud Security

Artificial Intelligence ups the cloud security risk stakes. Stay secure with a unified CNAPP that protects AI.

The adoption of Artificial intelligence (AI) increases the volume and variety of cloud data. In tandem, as they become more sophisticated, AI applications require more training datas to learn from and function effectively. This volume, variety and sensitivity makes protecting cloud data paramount to maintaining the integrity and security of your business's AI usage.

At their core, AI models are widely used and can involve highly sensitive data. And, like any cloud data that you produce—you're responsible for securing it. This includes securing the AI resources and data that are used for training and inference.

Risks to AI resources in the cloud

The OWASP Top 10 for LLM Applications outlines key AI risks that organizations should be aware of when assessing AI risks in the cloud.

- **Training data poisoning:** Manipulating data or fine-tuning to introduce vulnerabilities, backdoors, or biases, compromising the model's security and performance.
- **Supply chain vulnerabilities:** Compromises in training data and models from outdated software, susceptible pre-trained models, or insecure plugins.
- **Sensitive information disclosure:** Caused by excessive permissions and lack of access governance.
- **Excessive agency:** Over-functionality or excessive autonomy can lead to security risks. Limiting permissions and tracking user authorization are key to prevention.
- **Model theft:** Unauthorized access to LLM models, risking economic loss, reputation damage, and exposure of sensitive data.

Key AI security benefits in Tenable Cloud Security

- Get full analysis of your entire AI inventory
- Remediate AI resource vulnerabilities
- Safeguard AI training data
- Manage AI entitlements with ease
- Enforce AI configuration best practices

To combat these threats, organizations must ensure proper configuration, manage vulnerabilities on AI workloads and govern access to AI resources. For example, you must verify that your company's sensitive data isn't being used to train a public model and ensure that your company's internal AI/ML model is not being compromised by looking at the relationships between data, AI, access and vulnerability risks.

All of these dynamic considerations happen in conjunction with traditional security and compliance risks in the cloud that security teams already struggle to prioritize.

AI doesn't do silos. Neither should your security tools.

Because of its far reaching and critical impact, AI security risks have to be prioritized in context of your entire cloud exposure. Let's dive into how Tenable Cloud Security can help.

Expose and close AI risk in the cloud with Tenable Cloud Security

Tenable Cloud Security gives you complete visibility and intuitive analysis of AI resource and data in your multi-cloud environment. From training data, cloud services, AI workloads and deployed software components, Tenable Cloud Security unifies point solutions to provide context that exposes and closes emerging AI exposures. Findings are illustrated in the intuitive user dashboard and can be used for granular queries and to generate reports for simplified risk communication.

After detecting AI resources and software used by AI in multi-cloud environments, Tenable Cloud Security then labels those resources based on sensitivity and assigns them a severity. Sensitivity and severity ratings are based off of context from other Tenable Cloud Security findings such as access, vulnerability severity and configuration risk. This ensures personalized prioritizations and surface the most lethal exposures specific to your organization.

Tenable Cloud Security

Tenable Cloud Security is the actionable cloud security platform, rapidly exposing and closing priority security gaps caused by misconfigurations, risky entitlements and vulnerabilities. These weaknesses are the epicenter of cloud risk. Tenable is a world leader at isolating and eradicating these exposures at scale across infrastructure, workloads, identities, data and AI resources.

About Tenable

Tenable® is the exposure management company, exposing and closing the cybersecurity gaps that erode business value, reputation and trust. The company's AI-powered exposure management platform radically unifies security visibility, insight and action across the attack surface, equipping modern organizations to protect against attacks from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. By protecting enterprises from security exposure, Tenable reduces business risk for more than 44,000 customers around the globe. Learn more at www.tenable.com.

Contact Us:

Please email us at sales@tenable.com or visit tenable.com/contact

100424